

Connecting Multiple-unicast and Network Error Correction: Reduction and Unachievability

Wentao Huang

California Institute of Technology

Michael Langberg

University at Buffalo, SUNY

Joerg Kliewer

New Jersey Institute of Technology

Abstract—We show that solving a multiple-unicast network coding problem can be reduced to solving a single-unicast network error correction problem, where an adversary may jam at most a single edge in the network. Specifically, we present an efficient reduction that maps a multiple-unicast network coding instance to a network error correction instance while preserving feasibility. The reduction holds for both the zero probability of error model and the vanishing probability of error model. Previous reductions are restricted to the zero-error case. As an application of the reduction, we present a constructive example showing that the single-unicast network error correction capacity may not be achievable, a result of separate interest.

I. INTRODUCTION

Consider the problem that a source wishes to reliably communicate to a terminal over a network with point-to-point noiseless channels, in the presence of an adversary. The adversary is characterized by a collection \mathcal{A} of subsets of channels, so that it may choose an arbitrary $A \in \mathcal{A}$ and controls the channels in set A . Under the assumption that 1) all channels have uniform capacity and 2) \mathcal{A} is the collection of all subsets containing z channels, Yeung and Cai [1] show that the cut-set bound characterizes the network error correction capacity. Efficient capacity-achieving network error correction codes under this setting are proposed in [2]–[5].

In the settings that either channel capacities are not uniform or \mathcal{A} is arbitrary, determining the network capacity remains an open problem. For both cases it is shown that linear codes are not sufficient to achieve capacity [6], [7]. Capacity bounds and achievable strategies for network error correction with unequal channel capacities are studies in [6]. Achievable strategies for network error correction with non-uniform \mathcal{A} , i.e., \mathcal{A} includes subsets of different sizes, are studied in [8]–[10].

The single-source single-terminal network error correction problem with arbitrary \mathcal{A} is shown in a previous work of the authors [11] to be at least as hard as the multiple-unicast network coding problem (without adversarial errors), using the following reduction technique. For a general multiple-unicast network coding problem \mathcal{I} , a corresponding network error correction problem \mathcal{I}_c can be constructed, so that a rate is feasible with zero error in \mathcal{I} if and only if a corresponding rate is feasible with zero error in \mathcal{I}_c . Therefore, the problem of determining the zero-error feasibility of a rate in \mathcal{I} is reduced to the problem of determining the zero-error feasibility of a

rate in \mathcal{I}_c . Under the model that a vanishing probability of error is allowed, the connection between the feasibility in \mathcal{I} and \mathcal{I}_c is also studied in [11]. However, in this case the result therein is weaker, and has a gap so that the “if and only if” connection between \mathcal{I} and \mathcal{I}_c is broken. Hence for this case the reduction from \mathcal{I} to \mathcal{I}_c is *not* established.

In this paper, we close this gap and complete the reduction from multiple-unicast to network error correction under the vanishing-error model. For a general multiple-unicast network coding problem \mathcal{I} , we show that a corresponding network error correction problem \mathcal{I}_c can be constructed, so that a rate is feasible with vanishing error in \mathcal{I} if and only if a corresponding rate is feasible with vanishing error in \mathcal{I}_c . We construct \mathcal{I}_c in the same way as in [11]. However, compared to the (implicit) information-theoretic approach used in [11], we present a way to explicitly construct the network code for \mathcal{I} from the network code for \mathcal{I}_c . Furthermore, the new approach enables a stronger result, simplifies the proofs and generalizes the result of the zero-error model as a special case.

As there are connections between \mathcal{I} and \mathcal{I}_c for both zero-error feasibility and vanishing-error feasibility, it is natural to ask if the connection extends to the case of asymptotic feasibility. We answer this question negatively by constructing a counter-example. By applying our analysis to this example, we further show that the (single-source single-terminal) network error correction capacity is not achievable in general, which is a result of separate interest. Previous works [12], [13] have studied the unachievability of capacity for multiple-unicast networks and sum-networks, respectively.

II. MODELS

A. Multiple-unicast Network Coding

A network is a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where vertices represent network nodes and edges represent channels. Each edge $e \in \mathcal{E}$ has a capacity c_e , which is the number of bits that can be transmitted on e in one transmission. An instance $\mathcal{I} = (\mathcal{G}, \mathcal{S}, \mathcal{T}, B)$ of the *multiple-unicast network coding problem*, includes a network \mathcal{G} , a set of source nodes $\mathcal{S} \subset \mathcal{V}$, a set of terminal nodes $\mathcal{T} \subset \mathcal{V}$ and an $|\mathcal{S}|$ by $|\mathcal{T}|$ requirement matrix B . The (i, j) -th entry of B equals 1 if terminal j requires the information from source i and equals 0 otherwise. B is assumed to be a permutation matrix so that each source is paired with a single terminal. Denote by $s(t)$ the source required by terminal t . Denote $[n] \triangleq \{1, \dots, n\}$, and each source $s \in \mathcal{S}$ is associated with an independent message,

⁰This work has been supported in part by NSF grant CCF-1440014, CCF-1440001, CCF-1439465, and CCF-1321129.

represented by a random variable M_s uniformly distributed over $[2^{nR_s}]$. A *network code* of length n is a set of encoding functions ϕ_e for every $e \in \mathcal{E}$ and a set of decoding functions ϕ_t for each $t \in \mathcal{T}$. For each $e = (u, v)$, the encoding function ϕ_e is a function taking as input the signals received from the incoming edges of node u , as well as the random variable M_u if $u \in \mathcal{S}$. ϕ_e evaluates to a value in $[2^{nC_e}]$, which is the signal transmitted on e . For each $t \in \mathcal{T}$, the decoding function ϕ_t maps the tuple of signals received from the incoming edges of t , to an estimated message $\hat{M}_{s(t)}$ with values in $[2^{nR_{s(t)}}]$.

A network code $\{\phi_e, \phi_t\}_{e \in \mathcal{E}, t \in \mathcal{T}}$ is said to *satisfy* a terminal t under transmission $(m_s, s \in \mathcal{S})$ if $\hat{M}_{s(t)} = m_{s(t)}$ when $(M_s, s \in \mathcal{S}) = (m_s, s \in \mathcal{S})$. A network code is said to satisfy the multiple-unicast network coding problem \mathcal{I} with error probability ϵ if the probability that all $t \in \mathcal{T}$ are simultaneously satisfied is at least $1 - \epsilon$. The probability is taken over the joint distribution on $(M_s, s \in \mathcal{S})$. Formally, the network code satisfies \mathcal{I} with error probability ϵ if

$$\Pr_{(M_s, s \in \mathcal{S})} \left\{ \bigcap_{t \in \mathcal{T}} t \text{ is satisfied under } (M_s, s \in \mathcal{S}) \right\} \geq 1 - \epsilon.$$

For an instance \mathcal{I} of the multiple-unicast network coding problem, rate R is said to be *feasible* if $R_s = R, \forall s \in \mathcal{S}$, and for any $\epsilon > 0$, there exists a network code that satisfies \mathcal{I} with error probability at most ϵ . Rate R is said to be *feasible with zero error* if $R_s = R, \forall s \in \mathcal{S}$ and there exists a network code that satisfies \mathcal{I} with zero error probability. Rate R is said to be *asymptotically feasible* if for any $\delta > 0$, rate $(1 - \delta)R$ is feasible. The model assumes that all sources transmit information at equal rate. There is no loss of generality in this assumption as a varying rate source s can be modeled by several equal rate sources co-located at s .

B. Single-source Single-terminal Network Error Correction

An instance $\mathcal{I}_c = (\mathcal{G}, s, t, \mathcal{A})$ of the *single-source single-terminal network error correction problem* includes a network \mathcal{G} , a source node s , a terminal node t and a collection of subsets of channels $\mathcal{A} \subset 2^{\mathcal{E}}$ susceptible to errors. An error occurs in a channel if the output of the channel is different from the input. More precisely, the output of a channel e is the bitwise xor of the input signal and an error signal r_e . We say there is an error in channel e if r_e is not the zero vector. For a subset $A \in \mathcal{A}$ of channels, an A -error is said to occur if an error occurs in every channel in A . Since there is only a single source and a single terminal, in this problem we suppress the subscript and denote by M the random message of the source, by R the rate of M , and by \hat{M} the output of the decoder at t .

Denote by $\mathcal{R}_{\mathcal{A}}$ the set of *error patterns* $r = \{r_e\}_{e \in \mathcal{E}}$ that correspond to an A -error, for any $A \in \mathcal{A}$. A network code $\{\phi_e, \phi_t\}_{e \in \mathcal{E}}$ is said to *satisfy* \mathcal{I}_c under transmission m if $\hat{M} = m$ when $M = m$, regardless of the occurrence of any error pattern $r \in \mathcal{R}_{\mathcal{A}}$. A network code is said to satisfy problem \mathcal{I}_c with error probability ϵ if the probability that \mathcal{I}_c is satisfied is at least $1 - \epsilon$. The probability is taken over the distribution on the source message M . Note that our model targets the

worst-case scenario in the sense that if $M = m$ is transmitted and m is satisfied by the network code, then correct decoding is guaranteed regardless of the error pattern.

For a single-source single-terminal network error correction problem \mathcal{I}_c , rate R is said to be *feasible* if for any $\epsilon > 0$, there exists a network code that satisfies \mathcal{I}_c with error probability at most ϵ . Rate R is said to be *feasible with zero error* if there exists a network code that satisfies \mathcal{I}_c with zero error probability. Rate R is said to be *asymptotically feasible* if for any $\delta > 0$, rate $(1 - \delta)R$ is feasible. The capacity of \mathcal{I}_c is the supremum over all rates that are asymptotically feasible.

III. REDUCTION FROM MULTIPLE-UNICAST TO NETWORK ERROR CORRECTION

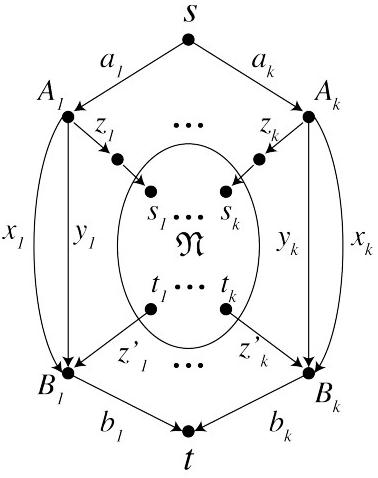


Fig. 1: In the single-unicast network error correction problem \mathcal{I}_c , the source s wants to communicate with the terminal t . \mathcal{N} is a general network with point-to-point noiseless channels. All edges outside \mathcal{N} (i.e., edges for which at least one of its end-points does not belong to \mathcal{N}) have unit capacity. There is at most one error in this network, and this error may occur at any edge except $\{a_i, b_i, 1 \leq i \leq k\}$. Namely, \mathcal{A} includes all singleton sets of a single edge in the network except $\{a_i\}$ and $\{b_i\}$, $i = 1, \dots, k$. Note that there are k parallel branches in total but only the first and the k -th branches are drawn explicitly. The multiple-unicast network coding problem \mathcal{I} is defined on the network \mathcal{N} , where the k source-destination pairs are $(s_i, t_i), i = 1, \dots, k$, and all channels are error-free.

The following theorem is the main result of this section.

Theorem 1. *Given any multiple-unicast network coding problem \mathcal{I} with source-destination pairs $\{(s_i, t_i), i = 1, \dots, k\}$, a corresponding single-source single-terminal network error correction problem $\mathcal{I}_c = (\mathcal{G}, s, t, \mathcal{A})$ in which \mathcal{A} includes sets with at most a single edge can be constructed as specified in Figure 1, such that rate k is feasible in \mathcal{I}_c if and only if unit rate is feasible in \mathcal{I} .*

The backward direction of the theorem, i.e., unit rate in \mathcal{I} implies rate k in \mathcal{I}_c , is simple and is proved in [11]. In the

remainder of this section we prove the forward direction of Theorem 1, i.e., the feasibility of rate k in \mathcal{I}_c implies the feasibility of unit rate in \mathcal{I} .

Suppose in \mathcal{I}_c a rate of k is achieved by a network code $\mathcal{C} = \{\phi_e, \phi_t\}_{e \in \mathcal{E}}$ with length n , and with a probability of error ϵ . Recall that M is the source message uniformly distributed over $\mathcal{M} = [2^{kn}]$, and \hat{M} is the output of the decoder at the terminal. Let $\mathcal{M}^{\text{good}} = \{m \in [2^{kn}] : \mathcal{C} \text{ satisfies } \mathcal{I}_c \text{ under transmission } m\}$ be the subset of messages that can be decoded correctly under any error pattern $r \in \mathcal{R}_{\mathcal{A}}$. Denote by $\mathcal{M}^{\text{bad}} = \mathcal{M} \setminus \mathcal{M}^{\text{good}}$, then for any $m \in \mathcal{M}^{\text{bad}}$, there exists an error pattern $r \in \mathcal{R}_{\mathcal{A}}$ such that $\hat{M} \neq m$ if $M = m$ and r occurs, i.e., a decoding error occurs. Because \mathcal{C} satisfies \mathcal{I}_c with error probability ϵ , it follows that $|\mathcal{M}^{\text{bad}}| \leq 2^{kn}\epsilon$ and thus $|\mathcal{M}^{\text{good}}| \geq (1 - \epsilon) \cdot 2^{kn}$.

We introduce some notation needed in the proof. In problem \mathcal{I}_c , under the network code \mathcal{C} , for $i = 1, \dots, k$, let $x_i(m, r) : \mathcal{M} \times \mathcal{R}_{\mathcal{A}} \rightarrow [2^n]$ be the signal received from channel x_i when $M = m$ and the error pattern r happens. Let $r = \mathbf{0}$ denotes the case that no error has occurred in the network. Let $x_i(m) = x_i(m, \mathbf{0})$, $\mathbf{x}(m, r) = (x_1(m, r), \dots, x_k(m, r))$ and $\mathbf{x}(m) = (x_1(m), \dots, x_k(m))$. We define functions $a_i, b_i, y_i, z_i, z'_i, \mathbf{a}, \mathbf{b}, \mathbf{y}, \mathbf{z}, \mathbf{z}'$ for problem \mathcal{I}_c in a similar way.

Notice that the set of edges a_1, \dots, a_k forms a cut-set from s to t , and so does the set of edges b_1, \dots, b_k . Therefore for any $m_1, m_2 \in \mathcal{M}^{\text{good}}$, $m_1 \neq m_2$, it follows from the decodability constraint that $\mathbf{a}(m_1) \neq \mathbf{a}(m_2)$ and $\mathbf{b}(m_1) \neq \mathbf{b}(m_2)$. Setting $\mathcal{B}^{\text{good}} = \{\mathbf{b}(m) : m \in \mathcal{M}^{\text{good}}\}$, it then follows from $|\mathcal{M}^{\text{good}}| \geq (1 - \epsilon) \cdot 2^{kn}$ that $|\mathcal{B}^{\text{good}}| \geq (1 - \epsilon) \cdot 2^{kn}$. Setting $\mathcal{B}^{\text{err}} = [2^n]^k \setminus \mathcal{B}^{\text{good}}$, it follows that $|\mathcal{B}^{\text{err}}| \leq 2^{kn}\epsilon$. We define $\mathcal{A}^{\text{good}}$ and \mathcal{A}^{err} similarly and so $|\mathcal{A}^{\text{good}}| \geq (1 - \epsilon) \cdot 2^{kn}$, $|\mathcal{A}^{\text{err}}| \leq 2^{kn}\epsilon$.

Let $\mathcal{M}(\hat{z}'_i, \hat{b}_i) = \{m \in \mathcal{M}^{\text{good}} : z'_i(m) = \hat{z}'_i, b_i(m) = \hat{b}_i\}$, we define a function $\psi_i : [2^n] \rightarrow [2^n]$ as:

$$\psi_i(\hat{z}'_i) = \arg \max_{\hat{b}_i} |\mathcal{M}(\hat{z}'_i, \hat{b}_i)| \triangleq \hat{b}_{i, \hat{z}'_i} \quad (1)$$

Function ψ_i will be useful later, when we design the network codes in \mathcal{I} . Intuitively, in the absence of adversarial errors, ψ_i estimates the signal transmitted on edge b_i given that the signal transmitted on edge z'_i is \hat{z}'_i . In the following we analyze how often will ψ_i make a mistake. Define $\mathcal{M}_i^{\psi} = \{m \in \mathcal{M}^{\text{good}} : \psi_i(z'_i(m)) \neq b_i(m)\}$. Notice that \mathcal{M}_i^{ψ} is the set of messages that, when they are transmitted by the source, ψ_i will make a mistake in guessing the signal transmitted on b_i . Lemma 1 shows that the size of this set is small.

Lemma 1. $|\mathcal{M}_i^{\psi}| \leq 2\epsilon \cdot 2^{kn}$.

We make the following combinatorial observation before proving Lemma 1. Lemma 2 is a variation of [11, Lemma 4]

Lemma 2. Let $\mathcal{M}(\hat{z}'_i) = \{m \in \mathcal{M}^{\text{good}} : z'_i(m) = \hat{z}'_i\}$, then for any $m_1, m_2 \in \mathcal{M}(\hat{z}'_i)$ such that $b_i(m_1) \neq b_i(m_2)$, there exists an element of \mathcal{B}^{err} that will be decoded by terminal t to either m_1 or m_2 .

Proof: Consider any $m_1, m_2 \in \mathcal{M}(\hat{z}'_i)$ such that $b_i(m_1) \neq b_i(m_2)$. Let r_1 be the error pattern that changes the signal on x_i to be $x_i(m_2)$, and let r_2 be the error pattern that changes the signal on y_i to be $y_i(m_1)$. Then if m_1 is transmitted by the source and r_1 happens, node B_i will receive the same inputs $(x_i(m_2), y_i(m_1), z'_i(m_1) = z'_i(m_2))$ as in the situation that m_2 is transmitted and r_2 happens. Therefore $b_i(m_1, r_1) = b_i(m_2, r_2)$, and so either $b_i(m_1, r_1) \neq b_i(m_1)$ or $b_i(m_2, r_2) \neq b_i(m_2)$ because by hypothesis $b_i(m_1) \neq b_i(m_2)$. Consider the first case that $b_i(m_1, r_1) \neq b_i(m_1)$, then the tuple of signals $(b_1(m_1, r_1), \dots, b_k(m_1, r_1)) = (b_1(m_1), \dots, b_i(m_1, r_1), \dots, b_k(m_1))$ will be decoded by the terminal to message m_1 because of the fact that $m_1 \in \mathcal{M}^{\text{good}}$ which is correctly decodable under any error pattern $r \in \mathcal{R}_{\mathcal{A}}$. Therefore this tuple of signals is an element of \mathcal{B}^{err} since it does not equals $\mathbf{b}(m_1) = (b_1(m_1), \dots, b_k(m_1))$ and it does not equal $\mathbf{b}(m)$, for any $m \neq m_1$, $m \in \mathcal{M}^{\text{good}}$, because otherwise it will be decoded by the terminal to m . Similarly in the latter case that $b_1(m_2, r_2) \neq b_1(m_2)$, then $(b_2(m_2, r_2), \dots, b_k(m_2, r_2)) = (b_2(m_2), \dots, b_i(m_2, r_2), \dots, b_k(m_2))$ is an element of \mathcal{B}^{err} and will be decoded by the terminal to m_2 . Therefore in both cases we are able to find an element of \mathcal{B}^{err} that will be decoded by the terminal to either m_1 or m_2 . ■

Proof (of Lemma 1): We can partition \mathcal{M}_i^{ψ} as

$$\mathcal{M}_i^{\psi} = \bigcup_{\hat{z}'_i} \left(\mathcal{M}(\hat{z}'_i) \setminus \mathcal{M}(\hat{z}'_i, \hat{b}_{i, \hat{z}'_i}) \right),$$

and so

$$|\mathcal{M}_i^{\psi}| = \sum_{\hat{z}'_i} \left(|\mathcal{M}(\hat{z}'_i)| - |\mathcal{M}(\hat{z}'_i, \hat{b}_{i, \hat{z}'_i})| \right). \quad (2)$$

Consider an arbitrary \hat{z}'_i and the set $\mathcal{M}(\hat{z}'_i)$. We define an iterative procedure as follows. Initialize $\mathcal{W} := \mathcal{M}(\hat{z}'_i)$. If there exist two messages $m_1, m_2 \in \mathcal{W}$ such that $b_i(m_1) \neq b_i(m_2)$, then delete both m_1, m_2 from \mathcal{W} . Repeat the operation until there does not exist $m_1, m_2 \in \mathcal{W}$ such that $b_i(m_1) \neq b_i(m_2)$.

After the procedure terminates, it follows that $|\mathcal{W}| \leq |\mathcal{M}(\hat{z}'_i, \hat{b}_{i, \hat{z}'_i})|$, otherwise by the definition of \hat{b}_{i, \hat{z}'_i} there must exist $m_1, m_2 \in \mathcal{W}$ such that $b_i(m_1) \neq b_i(m_2)$. Therefore at least $|\mathcal{M}(\hat{z}'_i)| - |\mathcal{M}(\hat{z}'_i, \hat{b}_{i, \hat{z}'_i})|$ elements are deleted from $\mathcal{M}(\hat{z}'_i)$. By Lemma 2, each pair of elements deleted corresponds to an element of \mathcal{B}^{err} . Also by Lemma 2 the elements of \mathcal{B}^{err} corresponding to different deleted pairs are distinct. Summing over all possible values of \hat{z}'_i , it follows that the total number of deleted pairs is smaller than the size of \mathcal{B}^{err} :

$$\begin{aligned} & \frac{1}{2} \sum_{\hat{z}'_i} \left(|\mathcal{M}(\hat{z}'_i)| - |\mathcal{M}(\hat{z}'_i, \hat{b}_{i, \hat{z}'_i})| \right) \\ & \leq \sum_{\hat{z}'_i} \# \text{ of pairs deleted from } \mathcal{M}(\hat{z}'_i) \\ & \leq |\mathcal{B}^{\text{err}}| = \epsilon \cdot 2^{kn}. \end{aligned} \quad (3)$$

Combining (2) and (3) we have $|\mathcal{M}_i^{\psi}| \leq 2\epsilon \cdot 2^{kn}$. ■

Next, let $\mathcal{M}(\hat{a}_i, \hat{b}_i) = \{m \in \mathcal{M}^{\text{good}} : a_i(m) = \hat{a}_i, b_i(m) = \hat{b}_i\}$, we define a function $\pi_i : [2^n] \rightarrow [2^n]$ as:

$$\pi_i(\hat{b}_i) = \arg \max_{\hat{a}_i} |\mathcal{M}(\hat{a}_i, \hat{b}_i)| \triangleq \hat{a}_{i, \hat{b}_i} \quad (4)$$

Function π_i will be useful later for designing the network codes in \mathcal{I} . Intuitively, in the absence of adversarial errors, π_i estimates the signal transmitted on edge a_i given that the signal transmitted on edge b_i is \hat{b}_i . In the following we analyze how often will π_i make a mistake. Define $\mathcal{M}_i^\pi = \{m \in \mathcal{M}^{\text{good}} : \pi_i(b_i(m)) \neq a_i(m)\}$. Notice that \mathcal{M}_i^π is the set of messages that, when they are transmitted by the source, π_i will make a mistake in guessing the signal transmitted on a_i . Lemma 3 shows that the size of this set is small.

Lemma 3. $|\mathcal{M}_i^\pi| \leq 3\epsilon \cdot 2^{kn}$.

We make the following combinatorial observation before proving Lemma 3. Lemma 4 is a variation of [11, Lemma 3].

Lemma 4. Define $\mathcal{M}(\hat{a}_i) = \{m \in \mathcal{M}^{\text{good}} : a_i(m) = \hat{a}_i\}$. If $|\{b_i(m) : m \in \mathcal{M}(\hat{a}_i)\}| = L$, then there exist $(L-1)|\mathcal{M}(\hat{a}_i)|$ distinct elements of \mathcal{B}^{err} such that each of them will be decoded by terminal t to some message $m \in \mathcal{M}(\hat{a}_i)$.

Proof: Assume for concreteness that $\{b_i(m) : m \in \mathcal{M}(\hat{a}_i)\} = \{\hat{b}_i^{(1)}, \dots, \hat{b}_i^{(L)}\}$, then there exist L messages $m_1, \dots, m_L \in \mathcal{M}(\hat{a}_i)$ such that $b_i(m_j) = \hat{b}_i^{(j)}$, $j = 1, \dots, L$. For $j = 1, \dots, L$, let r_j be the error pattern that changes the signal on z'_i to be $z'_i(m_j)$. Then if a message $m_0 \in \mathcal{M}(\hat{a}_i)$ is transmitted by the source and r_j happens, the node B_i will receive the same inputs $(x_i(m_0), y_i(m_0), z'_i(m_j))$ as in the situation that m_j is sent and no error happens. Therefore $b_i(m_0, r_j) = \hat{b}_i^{(j)}$, and so $|\{b(m_0, r_j)\}_{j \in [L]}| = |\{b_i(m_0, r_j)\}_{j \in [L]}| = L$. Since $m_0 \in \mathcal{M}^{\text{good}}$, it is correctly decodable under any error pattern $r \in \mathcal{R}_A$, and so all elements of $\{b(m_0, r_j)\}_{j \in [L]}$ will be decoded by the terminal to m_0 . Except the element $b(m_0)$, the other $L-1$ elements of $\{b(m_0, r_j)\}_{j \in [L]}$ are elements of \mathcal{B}^{err} . Sum over all $m_0 \in \mathcal{M}(\hat{a}_i)$ and the assertion is proved. ■

Proof (of Lemma 3): Define $\mathcal{A}_{i,1}^\pi = \{\hat{a}_i \in [2^n] : |\mathcal{M}(\hat{a}_i)| \leq \frac{1}{2}2^{(k-1)n}\}$, and $\mathcal{A}_{i,2}^\pi = \{\hat{a}_i \in [2^n] \setminus \mathcal{A}_{i,1}^\pi : |\{b_i(m) : m \in \mathcal{M}(\hat{a}_i)\}| > 1\}$. Then define $\mathcal{M}_{i,1}^\pi = \{m \in \mathcal{M}^{\text{good}} : a_i(m) \in \mathcal{A}_{i,1}^\pi\}$, and $\mathcal{M}_{i,2}^\pi = \{m \in \mathcal{M}^{\text{good}} : a_i(m) \in \mathcal{A}_{i,2}^\pi\}$. Notice that by construction $\mathcal{A}_{i,1}^\pi$ and $\mathcal{A}_{i,2}^\pi$ are disjoint, and $\mathcal{M}_{i,1}^\pi$ and $\mathcal{M}_{i,2}^\pi$ are disjoint. We claim that,

$$\mathcal{M}_i^\pi \subset \mathcal{M}_{i,1}^\pi \cup \mathcal{M}_{i,2}^\pi. \quad (5)$$

To prove the claim, consider any $m \in \mathcal{M}^{\text{good}}$ such that $m \notin \mathcal{M}_{i,1}^\pi \cup \mathcal{M}_{i,2}^\pi$. We will show that $\pi(b_i(m)) = a_i(m)$. Suppose for the sake of contradiction that $\pi(b_i(m)) = \hat{a}_i \neq a_i(m)$, then it follows that

$$\begin{aligned} |\mathcal{M}(\hat{a}_i, b_i(m))| &\stackrel{(a)}{>} |\mathcal{M}(a_i(m), b_i(m))| \\ &\stackrel{(b)}{=} |\mathcal{M}(a_i(m))| \stackrel{(c)}{>} \frac{1}{2}2^{(k-1)n}, \end{aligned} \quad (6)$$

where (a) is due to the definition of π , (b) is due to the fact that $m \notin \mathcal{M}_{i,2}^\pi$ and (c) is due to the fact that $m \notin$

$\mathcal{M}_{i,1}^\pi$. Let $\mathcal{M}(\hat{b}_i) = \{m' \in \mathcal{M}^{\text{good}} : b_i(m') = \hat{b}_i\}$, then $\mathcal{M}(\hat{a}_i, b_i(m)) \cup \mathcal{M}(a_i(m)) \subset \mathcal{M}(b_i(m))$. Since $\hat{a}_i \neq a_i(m)$, $\mathcal{M}(\hat{a}_i, b_i(m))$ and $\mathcal{M}(a_i(m))$ are disjoint, and it follows that $|\mathcal{M}(b_i(m))| \geq |\mathcal{M}(\hat{a}_i, b_i(m))| + |\mathcal{M}(a_i(m))| > 2^{(k-1)n}$. However, because $|\{(\hat{b}_1, \dots, \hat{b}_k) \in [2^n]^k : \hat{b}_i = b_i(m)\}| = 2^{(k-1)n}$, by the pigeonhole principle there must exist two messages $m_1, m_2 \in \mathcal{M}(b_i(m))$ such that $b(m_1) = b(m_2)$. This is a contradiction since the terminal cannot distinguish m_1 from m_2 . This proves $\pi(b_i(m)) = a_i(m)$ as well as (5).

We next bound the size of $\mathcal{M}_{i,1}^\pi$ and $\mathcal{M}_{i,2}^\pi$. For any $\hat{a}'_i \in \mathcal{A}_{i,1}^\pi$, by definition $\{(\hat{a}_1, \dots, \hat{a}_k) \in [2^n]^k : \hat{a}_i = \hat{a}'_i\} \setminus \{(\mathbf{a}(m) : m \in \mathcal{M}(\hat{a}'_i)\}$ is a subset of \mathcal{A}^{err} with size at least $\frac{1}{2}2^{(k-1)n}$. Therefore each element of $\mathcal{A}_{i,1}^\pi$ will contribute to at least $\frac{1}{2}2^{(k-1)n}$ distinct elements of \mathcal{A}^{err} . Hence $|\mathcal{A}_{i,1}^\pi| \cdot \frac{1}{2}2^{(k-1)n} \leq |\mathcal{A}^{\text{err}}| = \epsilon \cdot 2^{kn}$, and so $|\mathcal{A}_{i,1}^\pi| \leq 2\epsilon \cdot 2^n$. It then follows that $|\mathcal{M}_{i,1}^\pi| \leq \frac{1}{2}2^{(k-1)n} |\mathcal{A}_{i,1}^\pi| = \epsilon \cdot 2^{kn}$.

By Lemma 4, each elements of $\mathcal{A}_{i,2}^\pi$ will contribute to at least $\frac{1}{2}2^{(k-1)n}$ distinct elements in \mathcal{B}^{err} . Therefore $|\mathcal{A}_{i,2}^\pi| \cdot \frac{1}{2}2^{(k-1)n} \leq |\mathcal{B}^{\text{err}}| = \epsilon \cdot 2^{kn}$, and so $|\mathcal{A}_{i,2}^\pi| \leq 2\epsilon \cdot 2^n$. It then follows that $|\mathcal{M}_{i,2}^\pi| \leq 2^{(k-1)n} |\mathcal{A}_{i,2}^\pi| = 2\epsilon \cdot 2^{kn}$. Finally, by (5) we have $|\mathcal{M}_i^\pi| \leq |\mathcal{M}_{i,1}^\pi| + |\mathcal{M}_{i,2}^\pi| \leq 3\epsilon \cdot 2^{kn}$. ■

We are now ready to prove Theorem 1.

Proof (“ \Rightarrow ” part of Theorem 1): We show the feasibility of rate k in \mathcal{I}_c implies the feasibility of unit rate in \mathcal{I} .

Let $\{\phi_e, \phi_t\}_{e \in \mathcal{E}}$ be the network error correction code of length n that achieves rate k in \mathcal{I}_c , with probability of error ϵ . We assume that in this code edge z_i simply relays the signal from edge a_i . This is without loss of generality because for any network code that needs to process the signal on edge a_i to obtain the signal to be transmitted on edge z_i , it is equivalent to relay the signal on edge z_i and perform the processing work at the head node of edge z_i .

Let $\mathcal{E}_N \subset \mathcal{E}$ be the set of edges of the embedded graph \mathcal{N} . For the multiple-unicast problem \mathcal{I} , we define a length- n network code $\{\tau_e, \tau_{t_i} : e \in \mathcal{E}_N, i \in [k]\}$ as follows.

$$\begin{aligned} \tau_e &= \phi_e, \quad \forall e \in \mathcal{E}_N \\ \tau_{t_i} &= \phi_{z_i} \circ \pi_i \circ \psi_i \circ \phi_{z'_i}, \quad \forall i = 1, \dots, k. \end{aligned}$$

where \circ denotes function composition; ϕ_{z_i} and $\phi_{z'_i}$ are the encoding functions of edges z_i and z'_i in problem \mathcal{I}_c ; ψ_i is defined in (1); and π_i is defined in (4). In the following we show that $\{\tau_e, \tau_{t_i} : e \in \mathcal{E}_N, i \in [k]\}$ achieves unit rate in \mathcal{I} with probability of error upper bounded by $6ke$.

In problem \mathcal{I} , let M_i be the random message associated with source s_i , then $M_i, i = 1, \dots, k$ are i.i.d. uniformly distributed over $[2^n]$. Denote for short $\mathbf{M} = (M_1, \dots, M_k)$, then slightly abusing notations we denote by $\tau_{t_i}(\mathbf{M})$ the output of the decoder τ_{t_i} under transmission \mathbf{M} . The probability of decoding error is given by

$$\Pr \left\{ \bigcup_{i=1}^k \tau_{t_i}(\mathbf{M}) \neq M_i \right\},$$

where the probability is taken over the joint distribution of the random messages. Let $\mathbf{m} = (m_1, \dots, m_k)$ be the realization

of \mathcal{M} . We claim that if there exists a message m of problem \mathcal{I}_c (not to be confused with \mathbf{m} , a message of \mathcal{I}) such that $m \in \mathcal{M}^{\text{good}}$, $m \notin \mathcal{M}_i^\psi$, $m \notin \mathcal{M}_i^\pi$ and $\mathbf{m} = \mathbf{z}(m)$, then $\tau_{t_i}(\mathbf{m}) = m_i$. To prove the claim, suppose $\mathbf{m} = \mathbf{z}(m)$ is transmitted in \mathcal{I} . Notice that all edges in \mathcal{N} perform the same coding scheme in \mathcal{I} as in \mathcal{I}_c , therefore for terminal node t_i , by invoking the function $\phi_{\mathbf{z}'_i}$, it obtains $\mathbf{z}'_i(m)$. Then by the definition of \mathcal{M}_i^ψ , it follows that $\psi_i(\mathbf{z}'_i(m)) = b_i(m)$. And by the definition of \mathcal{M}_i^π , it follows that $\pi(\psi_i(\mathbf{z}'_i(m))) = a_i(m)$. Finally since $\mathbf{m} = \mathbf{z}(m)$, it follows that $\phi_{\mathbf{z}_i}(\pi(\psi_i(\mathbf{z}'_i(m)))) = \phi_{\mathbf{z}_i}(a_i(m)) = z_i(m) = m_i$.

Therefore $\tau_{t_i}(\mathbf{m}) = m_i$ if $\mathbf{m} \in \{\mathbf{z}(m) \in [2^n]^k : m \in \mathcal{M}^{\text{good}}, m \notin \mathcal{M}_i^\psi, m \notin \mathcal{M}_i^\pi\}$. The probability that τ_{t_i} makes an error, i.e., $\Pr\{\tau_{t_i}(\mathbf{M}) \neq M_i\}$, is upper bounded by the probability of the union of the following three events.

$$E_1 = \{\mathbf{M} = \mathbf{m} : \mathbf{m} \notin \{\mathbf{z}(m) \in [2^n]^k : m \in \mathcal{M}^{\text{good}}\}\}$$

$$E_2 = \{\mathbf{M} = \mathbf{m} : \mathbf{m} \in \{\mathbf{z}(m) \in [2^n]^k : m \in \mathcal{M}_i^\psi\}\}$$

$$E_3 = \{\mathbf{M} = \mathbf{m} : \mathbf{m} \in \{\mathbf{z}(m) \in [2^n]^k : m \in \mathcal{M}_i^\pi\}\}.$$

We upper bound the probability of E_1, E_2, E_3 , respectively.

$$\begin{aligned} \Pr\{E_1\} &= 1 - \frac{|\{\mathbf{z}(m) : m \in \mathcal{M}^{\text{good}}\}|}{2^{kn}} \\ &\stackrel{(d)}{=} 1 - \frac{|\mathcal{M}^{\text{good}}|}{2^{kn}} \leq 1 - \frac{(1 - \epsilon) \cdot 2^{kn}}{2^{kn}} = \epsilon, \end{aligned} \quad (7)$$

where (d) follows from the fact that $\mathbf{z}(m) = \mathbf{a}(m) \neq \mathbf{a}(m') = \mathbf{z}(m')$ for any $m, m' \in \mathcal{M}^{\text{good}}$, $m \neq m'$. By Lemma 1,

$$\Pr\{E_2\} = \frac{|\mathcal{M}_i^\psi|}{2^{kn}} \leq 2\epsilon. \quad (8)$$

And by Lemma 3, we have

$$\Pr\{E_3\} = \frac{|\mathcal{M}_i^\pi|}{2^{kn}} \leq 3\epsilon. \quad (9)$$

Combining (7), (8) and (9), it follows that

$$\Pr\{\tau_{t_i}(\mathbf{M}) \neq M_i\} \leq \Pr\{E_1\} + \Pr\{E_2\} + \Pr\{E_3\} \leq 6\epsilon.$$

Finally, by taking the union bound over the k terminals,

$$\Pr\left\{\bigcup_{i=1}^k \tau_{t_i}(\mathbf{M}) \neq M_i\right\} \leq 6k\epsilon.$$

Hence the probability of error is arbitrarily small and this establishes the feasibility of unit rate in \mathcal{I} . ■

The proof above suggests that the feasibility of rate k with error probability ϵ in \mathcal{I}_c implies the feasibility of unit rate with error probability $6k\epsilon$ in \mathcal{I} . By setting $\epsilon = 0$, we generalize the result in [11] regarding the zero-error model as a special case.

Corollary 1. *Given any multiple-unicast network coding problem \mathcal{I} with source-destination pairs $\{(s_i, t_i), i = 1, \dots, k\}$, a corresponding single-source single-terminal network error correction problem $\mathcal{I}_c = (\mathcal{G}, s, t, \mathcal{A})$ in which \mathcal{A} includes sets with at most a single edge can be constructed as specified in Figure 1, such that rate k is feasible with zero error in \mathcal{I}_c if and only if unit rate is feasible with zero error in \mathcal{I} .*

IV. UNACHIEVABILITY OF NETWORK ERROR CORRECTION CAPACITY

Theorem 1 and Corollary 1 suggest that there are strong “if and only if” connections between \mathcal{I}_c and \mathcal{I} for both zero-error feasibility and vanishing-error feasibility. It is natural to ask if this connection extends to the case of asymptotic feasibility, i.e., if it is true that rate k is asymptotically feasible in \mathcal{I}_c if and only if unit rate is asymptotically feasible in \mathcal{I} . We answer this question negatively by constructing a counter-example.

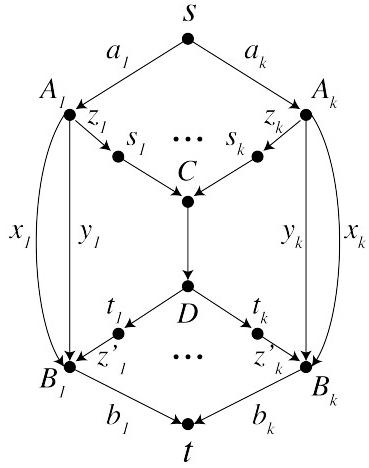


Fig. 2: Construction of \mathcal{I}_c and \mathcal{I} . In \mathcal{I}_c , the source is s and the terminal is t . \mathcal{A} includes all singleton sets of a single edge except $\{a_i\}$ and $\{b_i\}$, $i = 1, \dots, k$. In \mathcal{I} , the source-destination pairs are (s_i, t_i) , $i = 1, \dots, k$. All edges have unit capacity.

Theorem 2. *There exists a multiple-unicast network coding problem \mathcal{I} and a corresponding single-source single-terminal network error correction problem \mathcal{I}_c , constructed from \mathcal{I} as specified in Figure 2, such that rate k is asymptotically feasible in \mathcal{I}_c , but unit rate is not asymptotically feasible in \mathcal{I} .*

Proof: The construction of \mathcal{I} and the corresponding \mathcal{I}_c are shown in Figure 2. By the cut-set bounds, any rate larger than $1/k$ is not feasible in \mathcal{I} . This shows the second statement of the theorem.

We prove the first statement of the theorem by describing a network code with length n that achieves rate $k - k/n$ in \mathcal{I}_c . First divide the source message of rate $k - k/n$ into k pieces $M = (M_1, \dots, M_k)$, such that M_i , $i = 1, \dots, k$ are i.i.d. uniformly distributed over $[2^{n-1}]$. We denote $\phi_e : [2^{k(n-1)}] \rightarrow [2^n]$ as the encoding function¹ of edge e , which takes the source message M as input, and outputs the signal to be transmitted on e when there is no error in the network. For all $i = 1, \dots, k$, we let

$$\phi_{a_i}(M) = \phi_{x_i}(M) = \phi_{y_i}(M) = \phi_{z_i}(M) = \phi_{(s_i, C)}(M) = M_i$$

¹This is called the *global encoding function* in the context of network coding.

Furthermore, we let

$$\phi_{(C,D)}(M) = \phi_{(D,t_i)}(M) = \phi_{z'_i}(M) = \sum_{j=1}^k M_j, \quad \forall i = 1, \dots, k$$

where the summation is bitwise xor. Note that the edges $a_i, x_i, y_i, z_i, (s_i, C), (C, D), (D, t_i), z'_i$ each has a capacity to transmit n bits. But we only require each of them to transmit $n - 1$ bits. Hence each edge reserves one unused bit.

Node B_i , by observing the (possibly corrupted) signals received from edges x_i, y_i, z'_i , performs error correction in the following way. If the signal (of $n - 1$ bits) received from x_i equals the signal received from y_i , forward the signal to edge b_i , and then transmit one bit of 0 using the reserved bit. Otherwise, forward the signal received from z'_i to b_i , and then transmit one bit of 1 using the reserved bit.

Finally, terminal t recovers the source message in the following way. For $i = 1, \dots, k$, such that the reserved bit on b_i equals 0, decode the remaining $n - 1$ bits received from b_i as \hat{M}_i . If $\hat{M}_1, \dots, \hat{M}_k$ are all obtained in this way then decoding is completed. If two or more pieces of the \hat{M}_i 's are not obtained, then a decoding failure is declared. Otherwise, let \hat{M}_l be the unique piece that is not obtained, then subtract $\sum_{j=1, j \neq l}^k \hat{M}_j$ from the signal received from b_l , and decode the result as \hat{M}_l .

It remains to be shown that $\hat{M}_i = M_i, \forall i = 1, \dots, k$ regardless of the error patterns, and that a decoding failure will not be declared. Notice that the reserved bit on b_i equals 1 only if an error occurs to either x_i or y_i . Since there is at most a single error edge, for $i = 1, \dots, k$ there is at most one b_i with reserved bit 1. Therefore the decoder is able to obtain at least $k - 1$ pieces of $\hat{M}_1, \dots, \hat{M}_k$ during the first phase of decoding and will never declare failure. Next notice that if the reserved bit on b_i is 0, then $\hat{M}_i \neq M_i$ only if errors occur to both x_i and y_i . This is not possible by hypothesis and therefore $\hat{M}_i = M_i$ if the reserved bit on b_i is 0. Finally, suppose the reserved bit on b_i is 1, then an error must occur to either x_i or y_i , and so z'_i is not in error. Therefore $\hat{M}_i = \sum_{j=1}^k M_j - \sum_{j=1, j \neq i}^k \hat{M}_j = M_i$. This proves the correctness of decoding and the second statement of the theorem. ■

By applying the reduction result in Theorem 1 to the example constructed in Theorem 2, it follows that the same example shows the unachievability of single-unicast network error correction capacity.

Corollary 2. *There exists a single-source single-terminal network error correction problem whose capacity is not feasible.*

Proof: The construction of the network error correction problem \mathcal{I}_c is shown in Figure 2. By the cut-set bounds, the capacity of \mathcal{I}_c is upper bounded by k . By Theorem 2, rate k is asymptotically feasible in \mathcal{I}_c , and so the capacity of \mathcal{I}_c is k . Also by Theorem 2, unit rate is not feasible in \mathcal{I} , and so by Theorem 1, rate k is not feasible in \mathcal{I}_c . This shows that the capacity of \mathcal{I}_c is not feasible. ■

Corollary 2 suggests that although the network error correction capacity is (by definition) asymptotically feasible, in

general it may not be exactly feasible. This is in contrast to the scenario of network error correction with uniform \mathcal{A} , i.e., \mathcal{A} is the collection of all subsets containing z channels. In this case the network capacity can be achieved by linear codes. Unachievability of capacity is also studied for multiple-unicast networks [12] and sum networks [13]. For both cases example networks for which the capacity is not achievable are constructed using matroid theory.

V. CONCLUDING REMARKS

We show that determining the feasibility of a rate tuple in a multiple-unicast network coding problem can be efficiently reduced to determining the feasibility of a corresponding rate in a corresponding single-unicast network error correction problem, where an adversary may jam at most a single edge. Note that though our analysis assumes all source-destination pairs in the multiple-unicast transmit at equal rate, this restriction can be relaxed by modeling a varying rate source s as several equal rate sources co-located at s . Finally we apply the reduction to show the unachievability of single-unicast network error correction capacity.

We note that our results do not imply that finding the capacity of a multiple-unicast network coding problem can be reduced to finding the capacity of a single-unicast network error correction problem. Whether it is possible to construct such a reduction would be an interesting open problem.

REFERENCES

- [1] R. W. Yeung and N. Cai, "Network Error Correction, I: Basic Concepts and Upper Bounds," *Communications in Information & Systems*, vol. 6, no. 1, pp. 19–35, 2006.
- [2] Z. Zhang, "Linear network error correction codes in packet networks," *IEEE Trans. Info. Theory*, vol. 54, no. 1, pp. 209–218, Jan. 2008.
- [3] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Medard, and M. Effros, "Resilient Network Coding in the Presence of Byzantine Adversaries," *IEEE Trans. on Info. Theory*, vol. 54, no. 6, pp. 2596–2603, 2008.
- [4] D. Silva, F. R. Kschischang, and R. Kotter, "A Rank-Metric Approach to Error Control in Random Network Coding," *IEEE Trans. Info. Theory*, vol. 54, no. 9, pp. 3951–3967, 2008.
- [5] R. Koetter and F. R. Kschischang, "Coding for Errors and Erasures in Random Network Coding," *IEEE Trans. on Info. Theory*, vol. 54, no. 8, pp. 3579–3591, 2008.
- [6] S. Kim, T. Ho, M. Effros, and A. S. Avestimehr, "Network Error Correction With Unequal Link Capacities," *IEEE Trans. Info. Theory*, vol. 57, no. 2, pp. 1144–1164, Feb. 2011.
- [7] O. Kosut, L. Tong, and D. Tse, "Nonlinear Network Coding is Necessary to Combat General Byzantine Attacks," in *Allerton Conference on Communication, Control, and Computing*, 2009, pp. 593–599.
- [8] O. Kosut, L. Tong, and D. N. C. Tse, "Polytope codes against adversaries in networks," in *IEEE ISIT*, 2010, pp. 2423–2427.
- [9] D. Wang, D. Silva, and F. R. Kschischang, "Robust Network Coding in the Presence of Untrusted Nodes," *IEEE Trans. Info. Theory*, vol. 56, no. 9, pp. 4532–4538, 2010.
- [10] P. H. Che, M. Chen, T. Ho, S. Jaggi, and M. Langberg, "Routing for Security in Networks with Adversarial Nodes," in *IEEE NetCod*, 2013.
- [11] W. Huang, T. Ho, M. Langberg, and J. Kliewer, "Single-source/sink network error correction is as hard as multiple-unicast," in *Allerton Conference on Communication, Control, and Computing*, 2014.
- [12] R. Dougherty, C. Freiling, and K. Zeger, "Unachievability of network coding capacity," *IEEE Trans. Info. Theory*, vol. 52, no. 6, pp. 2365–2372, Jun. 2006.
- [13] B. K. Rai and B. K. Dey, "On Network Coding for Sum-Networks," *IEEE Trans. Info. Theory*, vol. 58, no. 1, pp. 50–63, Jan. 2012.